Несколько способов борьбы с торрентом на маршрутизаторе cisco. Варианты блокировки на сервере, который выступает в роли маршрутизатора, здесь не рассматриваю.

1 способ. Использование NBAR.

> Распознавание сетевых приложений (англ. Network Based Application Recognition, NBAR) — механизм, используемый в компьютерных сетях для распознавания потока данных (dataflow) по первому переданному пакету. Источник.

Переходим в привилегированный режим

```
>en
```

Смотрим в привилегированном режиме есть ли протокол bittorrent и с какими портами он работает.

```
#sh ip nbar port-map.
..
port-map bittorrent udp 3724
port-map bittorrent tcp 3724 1080 6969 6881 6882 6883 6884 6885 6886
6887 6888 6889
..
```

Переходим в режим глобальной конфигурации

```
#conf t
```

Создаем класс для того, чтобы описать класс трафика. И ставим match-all. match-any или match-all соответственно логическое ИЛИ или И. Полезно когда несколько команд match в классе используется, но мы будем использовать одну команду match только,а именно..match protocol bittorrent

```
(config)#class-map match-all torrentzz
(config-cmap)#match protocol bittorrent
```

выходим в режим глобального конфигурирования

```
(config-cmap)#exit
```

Создаем политику трафика. Добавляем наш класс. Прописываем действие drop. т.е. весь трафик, который будет удовлетворятся политики будет отбрасывает.

```
(config)#policy-map DROP_TORRENTZZ
(config-pmap)# class torrentzz
(config-pmap-c)#drop
```

Помимо drop есть еще некоторые варианты:
police cir 8000 bc 8000 — ограничение скорости входящей и исходящей в битах
conform-action action — действие при удовлетворении ограничениям
exceed-action action — действие при выходе за ограничения
Возможные варианты действий:
drop – уничтожить
transmit — передать
set-dscp-transmit – пометить пакет

Поехали дальше)

Переходим во внешний интерфейс и вешаем нашу политику на него.

```
(config)#int gi0/0
(config-if)#service-policy input DROP_TORRENTZZ
```

Посмотреть результат работы политики

```
#sh policy-map int gi0/0
```

Да. Данный способ так себе. Так как порты меняются и шифрованный трафик проходит мимо политики.

2 способ. ACL.
Суть проста. Разрешить только нужные порты (например только 80, 22), а остальные заблокировать.

Переходим в привилегированный режим

```
>en
```

Переходим в режим глобальной конфигурации

```
#conf t
```

Создаем расширенный ACL с указанием разрешенных портов.
permit — разрешить
deny — запретить
tcp/udp — с проверкой установления соединения / без (лучше отдельно почитать про IP,TCP,UDP)
eq — конкретный порт
gt — выше порта
lt — ниже порта
any any — от любых хостов любым хостам передача данных.

```
(config)#access-list 102 permit tcp any any eq 80
(config)#access-list 102 permit tcp any any eq 22
(config)#access-list 102 deny ip any any
```

осмотреть все списки можно так

```
#sh access-lists
```

Переходим во внешний интерфейс и вешаем наш ACL на него. in/out — входящий/исходящий трафик.

```
(config)#int gi0/0
(config)#access-list
(config-if)#ip access-group 102 in
```

Данный способ чуть поможет, но торрент может бегать и по 80 порту, или по любому другому открытому. Поэтому смотрим 3 способ)

3 способ.
Объяснить качальщику, что так делать нельзя. А как будете объяснять…это уже на свое усмотрение))